DEFENSORIA PÚBLICA
ESTADO DO RIO GRANDE DO SUL

RESOLUÇÃO DPGE Nº 07/2018

Institui a Política de Segurança da Informação e das Comunicações no âmbito da Defensoria Pública do Estado do Rio Grande do Sul e dá outras providências.

O **DEFENSOR PÚBLICO-GERAL DO ESTADO**, no uso de suas atribuições legais, conferidas pelo artigo 100 da Lei Complementar nº 80/1994 e pelo artigo 11, inciso II, da Lei Complementar Estadual nº 14.130/2012;

CONSIDERANDO as boas práticas em segurança da informação preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013;

CONSIDERANDO a necessidade de estabelecer princípios e diretrizes no que tange às ações de segurança da informação e das comunicações no âmbito da Instituição;

CONSIDERANDO as diretrizes estabelecidas no Planejamento Estratégico e no Plano Diretor de Tecnologia da Informação;

CONSIDERANDO o decidido pelo Conselho de Tecnologia da Informação na reunião III/2017 realizada em 31 de outubro de 2017;

CONSIDERANDO o que foi decidido nos autos do Expediente Administrativo Eletrônico nº 17/3000-0000037-1;

RESOLVE editar a seguinte **RESOLUÇÃO**:

Capítulo I – Disposições Gerais

Art. 1º Fica instituída a Política de Segurança da Informação e das Comunicações com finalidade de estabelecer os princípios e diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio, pelos sistemas de informação, devendo, obrigatoriamente, serem observados na definição de regras operacionais e procedimentos no âmbito da Defensoria Pública do Estado do Rio Grande do Sul.

§ 1º A Política tem como objetivo estabelecer normas, procedimentos, mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos custodiados e gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confidencialidade das informações na Defensoria e observando os princípios constitucionais, administrativos e a legislação vigente.

§ 2º O estabelecido nesta Política aplica-se a todos os membros, servidores e estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da Defensoria.

Publicado no
DED de 21 / 05 / 2018
Pág. nº 14-27
DEFENSORIA PÚBLICA
ESTADO DO RIO GRANDE DO SUL

DEFENSORIA PÚBLICA-GERAL DO ESTADO
Rua Sete de Setembro, 666, 7º andar
Centro Histórico – Porto Alegre/RS
Brasil – CEP: 90010-190
Telefone: (0xx51) 3210-9415

Capítulo II – Conceitos e Definições

Art. 2º Para os fins desta Política, considera-se:

I – Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação da Instituição;

II – Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III – Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

IV – Ativo de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V – Ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação;

VI – Classificação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

VII – Comitê de Governança de Tecnologia da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de governança de TI no âmbito da Defensoria;

VIII – Comitê de Segurança da Informação e das Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito da Defensoria;

IX – Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

X – Conselho de Tecnologia da Informação: grupo de pessoas da alta administração com a responsabilidade de encaminhar ações e aprovar diretrizes e políticas, para subsidiar o planejamento, a execução e a gestão da tecnologia da informação da instituição;

XI – Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XII – Custodiante: responsável por armazenar e preservar as informações que não lhe pertencem, refere-se a qualquer indivíduo ou estrutura da Defensoria que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação comunicadas pelos proprietários dos ativos de informação;

XIII – Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XIV – Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XV – Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XVI – Evento: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da Política de Segurança da Informação e das Comunicações ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

XVII – Gestor de Segurança da Informação e das Comunicações: servidor responsável pelas ações de segurança da informação e das comunicações no âmbito da Defensoria;

XVIII – Incidente de Segurança da Informação: indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores;

XIX – Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XX – Informação custodiada: informação sob a guarda e responsabilidade de alguém;

XXI – Integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino;

XXII – Política de Segurança da Informação e das Comunicações: documento aprovado pelo Defensor Público-Geral do Estado, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e das comunicações;

XXIII – Proprietário da Informação: pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade cada uma se enquadra;

XXIV – Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXV – Risco: efeito da incerteza sobre os objetivos de segurança da informação e é associado com o potencial que as ameaças explorarão vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização;

XXVI – Segregação de funções: consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum usuário detenha poderes e atribuições em desacordo com este princípio;

XXVII – Segurança da Informação e das Comunicações: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

XXVIII – Sigilo: segredo de conhecimento restrito a pessoas credenciadas e protegido contra revelação não autorizada;

XXIX – Usuários: membros, servidores, terceirizados, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação;

XXX – Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Capítulo III – Princípios e Diretrizes

Art. 3º A Política de Segurança da Informação e das Comunicações, as normas complementares e procedimentos devem obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública, além dos princípios da segurança da informação de disponibilidade, integridade e confidencialidade.

Art. 4º São diretrizes gerais da Política de Segurança da Informação e das Comunicações:

I – Definir critérios de tratamento e classificação dos dados, informações, comunicações e conhecimentos custodiados e produzidos pela Defensoria, com intuito de assegurar a disponibilidade, integridade e confidencialidade durante todo o seu ciclo de vida;

II – Implementar estratégias para preservar a continuidade dos serviços de TI em situações de crise, permitindo minimizar possíveis impactos nas atividades institucionais da Defensoria;

III – Estabelecer um processo de gestão de riscos relativos à segurança da informação e das comunicações com vistas a minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança;

IV – Identificar os usuários de maneira única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

V – Elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de segurança da informação em vigor;

VI – Implementar controles de acesso lógico e físico no âmbito da Tecnologia da Informação, sendo a concessão de direitos feita mediante aprovação formal e seguindo ao critério do menor privilégio, no qual os usuários têm permissão limitada aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

VII – Garantir, sempre que possível, a segregação de funções, por meio da participação de mais de uma pessoa ou equipe nos processos, com intuito de promover o controle interno e a redução de riscos;

VIII – Definir regras claras e precisas de uso dos ativos de informação institucionais, com o objetivo de evitar o uso pelos agentes públicos para fins particulares;

IX – Identificar, monitorar, comunicar e tratar os incidentes de segurança da informação de forma a impedir a interrupção das atividades e não afetar o alcance dos objetivos estratégicos;

X – Divulgar e disseminar por meio de programas permanentes de conscientização para todos os usuários questões sobre segurança da informação e das comunicações, o conteúdo desta Política e demais normas que a apoiam;

XI – Promover a melhoria contínua nos processos e controles de gestão da segurança da informação e das comunicações, observando as boas práticas, normas e procedimentos recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões relacionados a esse tema.

Capítulo IV – Competências e Responsabilidades

Art. 5º O Gabinete do Defensor Público-Geral do Estado será responsável por:

I – Assegurar que a implementação dos controles de segurança da informação e das comunicações tenha uma coordenação e permeie toda a organização;

II – Assegurar os recursos necessários para a implementação e gestão da Política de Segurança da Informação e das Comunicações da Defensoria.

Art. 6º São atribuições do Conselho de Tecnologia da Informação:

I – Definir critérios para auditoria periódica destinada a aferir o cumprimento da Política de Segurança da Informação e das Comunicações da Defensoria, suas normas complementares e procedimentos;

II – Aprovar a Política de Segurança da Informação e das Comunicações submetendo a mesma ao Defensor Público-Geral do Estado;

III – Aprovar e publicar as normas complementares e procedimentos relativos à segurança da informação, por ato do presidente do Conselho de Tecnologia da Informação;

IV – Referendar as decisões emanadas do Comitê de Segurança da Informação e das Comunicações;

V – Designar o Gestor de Segurança da Informação e das Comunicações;

VI – O Gestor de Segurança da Informação e das Comunicações será nomeado por portaria do Defensor Público-Geral do Estado.

Art. 7º Fica criado o Comitê de Segurança da Informação e das Comunicações da Defensoria Pública do Estado do Rio Grande do Sul, que terá como escopo a gestão da segurança da informação da Instituição, sendo de sua competência:

I – Assessorar na implementação das ações de segurança da informação e das comunicações no âmbito da Defensoria;

II – Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e das comunicações;

III – Propor normas complementares e procedimentos relativos à segurança da informação e das comunicações, em conformidade com as legislações existentes sobre o tema;

IV – Propor alterações à Política de Segurança da Informação e das Comunicações;

V – Revisar a Política de Segurança da Informação e das Comunicações, bem como as normas complementares e procedimentos, no prazo estabelecido nesta Política;

VI – Designar a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

Art. 8º O Comitê de Segurança da Informação e das Comunicações será constituído por:

I – Defensor Público indicado pelo Conselho de Tecnologia da Informação e das Comunicações, que o presidirá;

II – Diretor de Tecnologia da Informação;

III – Gestor da Segurança da Informação e das Comunicações;

IV – Até 02 (dois) servidores indicados pelo Diretor de Tecnologia da Informação;

§ 1º Os membros do comitê serão nomeados por portaria do Defensor Público-Geral do Estado;

§ 2º Excepcionalmente, até a formalização da portaria prevista no parágrafo anterior, o Comitê de Segurança da Informação será formado pelos membros do Comitê de Governança de Tecnologia da Informação e das Comunicações, além do Gestor de Segurança da Informação;

Art. 9º O Comitê de Segurança da Informação e das Comunicações reunir-se-á, de forma ordinária, trimestralmente, mediante convocação do seu Presidente, sem prejuízo da realização de reuniões extraordinárias.

Parágrafo único. As reuniões do Comitê serão precedidas do encaminhamento das respectivas pautas, com antecedência mínima de 48 horas da data aprazada, a todos os que dela devam participar.

Art. 10. O Comitê de Segurança da Informação irá propor ao Conselho de Tecnologia da Informação, normas complementares e procedimentos destinados a disciplinar e proteger o uso da informação no âmbito da Defensoria, complementando os controles de Gestão de Segurança da Informação contidos na Política de Segurança da Informação e das Comunicações, sobre os temas julgados relevantes, tais como:

I – Classificação e Tratamento da Informação;

II – Gestão de Ativos de Informação;

III – Gestão de Riscos de Segurança da Informação;

IV – Gestão de Continuidade dos Serviços de TI;

V – Gestão de Incidentes de Segurança da Informação;

VI – Segurança da Informação em Recursos Humanos;

VII – Segurança da Informação nas Contratações, Convênios, Acordos e Instrumentos Congêneres;

VIII – Segurança da Informação no Desenvolvimento de Sistemas;

IX – Auditoria e Conformidade;

X – Controles de Acesso Físico e aos Sistemas;

XI – Uso dos Recursos Computacionais;

XII – Uso de Correio Eletrônico;

XIII – Uso e Acesso à Internet e Intranet.

Art. 11. São atribuições do Gestor de Segurança da Informação e das Comunicações:

I – Promover cultura de segurança da informação e comunicações;

II – Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III – Propor recursos necessários às ações de segurança da informação;

IV – Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

V – Coordenar as reuniões do Comitê de Segurança da Informação e das Comunicações;

VI – Coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETRIS;

VII – Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VIII – Propor, ao Comitê de Segurança da Informação e das Comunicações, normas complementares e procedimentos relativos à segurança da informação no âmbito da Defensoria;

IX – Propor, ao Comitê de Segurança da Informação e das Comunicações, modificações à Política de Segurança da Informação e das Comunicações.

Art. 12. São atribuições da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETRIS:

I – Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II – Promover a recuperação de sistemas, quando da quebra da segurança da informação;

III – Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação e avaliando condições de segurança de redes por meio de verificações de conformidade;

IV – Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V – Analisar ataques e intrusões na rede da Defensoria;

VI – Executar as ações necessárias para tratar quebras de segurança;

VII – Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

Art. 13. São deveres dos usuários:

I – Conhecer e cumprir os princípios, diretrizes e responsabilidades desta Política e demais normas complementares e procedimentos relacionados;

II – Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;

III – Comunicar os incidentes que afetam a segurança dos ativos de informação à ETRIS.

Capítulo V – Penalidades

Art. 14. O não cumprimento das determinações da Política de Segurança da Informação e das Comunicações, das normas complementares e procedimentos sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos da Defensoria;

Art. 15. O descumprimento das disposições constantes nesta Política, nas normas complementares e procedimentos sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

Art. 16. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos desta Política, fica sujeito à aplicação das penalidades previstas na Leis Complementares, 11.795/02 e 10.098/94, e na legislação pertinente;

Capítulo VI – Da Atualização

Art. 17. Esta Política de Segurança da Informação e das Comunicações, bem como as normas complementares e procedimentos elaborados a partir dela, deverão ser revisados e atualizados periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Capítulo VII – Das Referências Legais e Normativas

Art. 18. Esta Política têm como referências legais e normativas os seguintes dispositivos:

I – Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso a Informação;

II – Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

III – Lei n° 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

IV – Lei nº 8.159, de 08 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e alterações legais;

V – Decreto nº 49.111, de 16 de maio de 2012, que regulamenta, no âmbito da Administração Pública Estadual, a Lei Federal nº 12.527/2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, cria a Comissão Mista de Reavaliação de Informações da Administração Pública Estadual – CMRI/RS, e dá outras providências;

VI – Decreto nº 53.164, de 10 de agosto de 2016, que regulamenta, no âmbito da Administração Pública Estadual, os procedimentos para a classificação de informações, prevista na Lei Federal nº 12.527, de 18 de novembro de 2011, e no Decreto nº 49.111, de 16 de maio de 2012, e dá outras providências;

VII – Decreto nº 52.808, de 18 de dezembro de 2015, que reorganiza o Sistema de Arquivos do Estado do Rio Grande do Sul – SIARQ/RS;

VIII – Resolução DPGE nº 13/2016;

IX – Norma NBR/ISO/IEC 27.002/2013 – Código de prática para controles de segurança da informação;

X – Norma NBR/ISO/IEC 27.001/2013 – Sistema de gestão de segurança da informação;

XI – Norma NBR/ISO/IEC 27.005/2011 – Gestão de riscos de segurança da informação;

XII – Norma NBR/ISO/IEC 22.301/2013 – Sistema de gestão de continuidade dos negócios.

Capítulo VIII – Disposições Finais

Art. 19. As questões interpretativas e os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e das Comunicações.

Art. 20. Esta Resolução entra em vigor na data de sua publicação.

Registre-se.
Publique-se.

Porto Alegre, 11 de maio de 2018.

CRISTIANO VIEIRA HEERDT
Defensor Público-Geral do Estado

Publicado no
DED de 21 / 05 / 2018
Pág. nº 14 - 27

DEFENSORIA PÚBLICA-GERAL DO ESTADO
Rua Sete de Setembro, 666, 7º andar
Centro Histórico – Porto Alegre/RS
Brasil – CEP: 90010-190
Telefone: (0xx51) 3210-9415